Rector's Decree No. 09/2024

Cybersecurity Policy

I. Introductory provisions

1) The Cybersecurity Policy sets out and elaborates the requirements for cybersecurity according to Act No. 181/2014 Sb., on cybersecurity and on changes of related acts, as amended (hereinafter the *"Cybersecurity Act"*), and decree No. 82/2018 Sb., on security measures, cybersecurity incidents, reactive measures, submission requirements in the field of cybersecurity and data disposal (hereinafter the *"Cybersecurity Decree"*) at the University of Hradec Králové (hereinafter the *"UHK"*).

2) The purpose of this Rector's Decree is to declare and approve the basic principles of security for the operation of important information systems (hereinafter *"IIS"*) at the UHK. The Cybersecurity Policy is the starting document for the security policies and security documentation implementing the cybersecurity of the IIS at the UHK.

II. Binding effect

1) The obligation to comply with the Cybersecurity Act is imposed on authorities or persons referred to in Section 3 of the Cybersecurity Act. That authority or person shall cooperate and act at least to the extent provided for in the Cybersecurity Act. According to Section 3(e) of the Cybersecurity Act, the UHK is the administrator and operator of the IIS.

2) The UHK as the administrator and operator of the IIS implements and carries out security measures, reports contact data and cybersecurity events and incidents at least to the extent specified in the Cybersecurity Act. The National Cyber and Information Security Agency (hereinafter also referred to as the *"NCISA"*) monitors compliance with the Cybersecurity Act and implementing decrees.

3) This decree and related security policies are binding for all employees and students of the UHK.

III. Scope

1) To ensure and support cybersecurity, the UHK is guided by this Rector's Decree which:
   a) Describes and explains the security of the IIS UHK;
   b) Describes the roles and competences for ensuring and executing the cybersecurity agenda at the UHK;
   c) Sets the security strategy;
   d) Sets the objectives and procedures of the security strategy;
   e) Outlines the structure of security policies and security documentation;
   f) Includes ways to revise this Rector's Decree.
2) The issue of cybersecurity covers the entire structure of the UHK in all locations of its activity, including cooperating organizations that come into contact with the IIS UHK.
3) Cybersecurity affects all identified assets of the UHK to a degree and extent appropriate to the importance of the asset.

IV. Roles and competences

1) The position of a Cybersecurity Manager (hereinafter the *"CS Manager"*) and an advisory Cybersecurity Committee (hereinafter the *"CS Committee"*) have been established to ensure and execute the cybersecurity agenda at the UHK.
2) The CS Manager performs tasks arising from the duties of the Cybersecurity Manager under the Cybersecurity Act and the Cybersecurity Decree. All activities of the CS Manager are described in the Rector's Decree regulating the position of the *Cybersecurity Manager of the UHK*.[1]
3) The CS Committee is established by the Rector of the UHK to ensure the management of cybersecurity at the UHK within the meaning of the Cybersecurity Act and the Cybersecurity Decree. All activities of the CS Committee are described in the Rector's Decree regulating the status of the *Cybersecurity Committee of the UHK*.[2]

[1] At the time of this Decree issue, the position of the Cybersecurity Manager is governed by the Rector's Decree No. 17/2023.
[2] At the time of this Decree issue, the status of the Cybersecurity Committee is governed by the Rector's Decree No. 16/2023.

V. Security Strategy

1) A security management strategy is being implemented for the security of the IIS UHK. The implementation of the security management strategy is based on the identification and assessment of risks of individual assets used for the operation of the IIS.

2) According to the Cybersecurity Act, the implementation of the security management strategy is ensured by the following security measures:

   a) Organisational measures;

   b) Technical measures.

3) According to the Cybersecurity Act, organisational measures include:

   a) Information security management system;

   b) Risk management;

   c) Security policy;

   d) Organisational security;

   e) Setting security requirements for suppliers;

   f) Asset management;

   g) Human resource security;

   h) Management of the operation and communications of the critical information infrastructure or significant information system;

   i) Management of access of persons to the critical information infrastructure or to major information systems;

   j) Acquisition, development and maintenance of critical information infrastructure and major information systems;

   k) Management of cybersecurity events and cybersecurity incidents;

   l) Management of business continuity;

   m) Control and audit of the critical information infrastructure and major information systems.

4) According to the Cybersecurity Act, technical measures include:

   a) Physical security;

   b) A tool to protect the integrity of communication networks;

   c) A tool to verify user identity;

   d) A tool to manage access permissions;

   e) A tool to protect against malicious code;

f) A tool to record activities of the critical information infrastructure and important information systems, their users and administrators;

g) A tool to detect cybersecurity events;

h) A tool to collect and evaluate cybersecurity events;

i) Application security;

j) Cryptographic means;

k) A tool to ensure the level of availability of information;

l) Safety of industrial and control systems.

VI. Objectives and procedures of the security strategy

1) The aim of the security strategy is to ensure that cybersecurity is implemented properly at the UHK and that the operation of the IIS is not in any way restricted or disrupted through breaches of availability, confidentiality or integrity. Internal measures and procedures to meet the basic objectives of the security strategy at the UHK include prevention, detection and response.

2) Prevention means preventive measures reducing identified risks, depending on their technical and economic feasibility. The *risk analysis* including the draft of the *Risk Management Plan* is prepared by the CS Manager regularly once a year and irregularly in case of significant changes in the setup and configuration of the IIS UHK. Technical measures are used as a priority; organizational measures are chosen only if an equivalent technical measure does not exist or cannot be used under the given configuration or economic conditions.

3) Detection consists in the introduction of organisational and technical measures to ensure the timely detection of security events and security incidents in the IIS UHK. All systems must record important user activity and functionality of their own SW and HW resources. Acceptable risk that is not addressed by appropriate preventive measures must be ensured by a high-quality set of measures for the detection of security events and incidents.

4) Response means a specific procedure for the investigation, resolution and eventual recovery of the IIS UHK, using primarily organisational measures with some degree of technical resources.

5) The procedures to ensure the security strategy include:
   a) Ensuring compliance with legislation;
   b) Ensuring uniform protection of the IIS according to the requirements of the legislation;
   c) Ensuring adequate resources (personnel, technical and financial) for cybersecurity;
   d) Implementing security technologies and their continuous updating and modernisation;
   e) Ensuring the ability to manage security events and incidents;
   f) Ensuring an adequate level of confidentiality, integrity and availability;
   g) Formalising the processes and procedures;
   h) Determining responsibilities;
   i) Increasing the level of security awareness of employees.
6) The UHK supports the stated objectives and procedures of the security strategy and considers the strategy of continuous cybersecurity assurance as an integral part of its own management processes.

VII. Structure of safety documentation

1) Within the cybersecurity management, the UHK maintains the following documentation system regulating individual aspects of cybersecurity at the UHK:
   a) Security policies;
   b) Safety documentation.
2) Security policies are available at **uhk.cz/kyberbezpecnost-politiky** and are issued in the following mandatory scope:
   a) Information security management system policy;
   b) Asset management policy;
   c) Organizational security policy;
   d) Supplier management policy;
   e) Human resources security policy;
   f) Traffic and communications management policy;
   g) Access control policy;
   h) Safe user behaviour policy;

i) Backup and recovery and long-term storage policy;

j) Secure information transfer and exchange policy;

k) Technical vulnerability management policy;

l) Policy on the safe use of mobile devices;

m) Acquisition, development and maintenance policy;

n) Privacy policy;

o) Physical security policy;

p) Communication network security policy;

q) Malicious code protection policy

r) Policy on the deployment and use of cybersecurity event detection tools;

s) Policy on the use and maintenance of the tool for cybersecurity event collection and assessment;

t) Policy on the secure use of cryptographic protection;

u) Change management policy;

v) Cybersecurity incident management policy;

w) Business continuity management policy.

3) Safety documentation is kept in the following mandatory scope:

a) Cybersecurity audit report;

b) Information security management system review report;

c) Methodology for asset identification and assessment and for risk identification and assessment;

d) Asset and risk assessment report;

e) Declaration of applicability;

f) Risk management plan;

g) Security awareness development plan;

h) Change records;

i) Overview of generally binding legislation, internal regulations and other regulations and contractual obligations.

VIII. Security policy review

1) The Cybersecurity Policy shall be reviewed at least once a year. The CS Manager is responsible for the review of this Rector's Decree. The final version of the document is approved by the KB Committee.
2) A revision of the Cybersecurity Policy:
   a) Is focused on security policies and security documentation;
   b) Is aimed at ensuring compliance of technical and organisational measures with security policies and security documentation;
   c) Includes suggestions for options to improve cybersecurity at the UHK;
   d) Includes proposals for changes in the IIS operated at the UHK.

IX. Final provisions

This Rector's Decree shall enter into force and effect on the date of its signature.

In Hradec Králové on 13 June 2024

Prof. Ing. Kamil Kuča, Ph.D.
Rector